REMARKS/ARGUMENTS

In this amendment, claims 1, 8, and 10-15 are amended to elaborate on existing limitations. No claims are canceled or added. Thus, after entry of this amendment, claims 1-15 remain pending. Note that the paragraph numbers cited herein refer to the version of the specification found on PAIR.

Interview Request

Applicant respectfully requests an interview to discuss the rejections and objections in the Office Action.

Claim Rejections under 35 USC § 101, Non-Statutory Subject Matter

Claim 14 is rejected as being directed to non-statutory subject matter. The Office Action asserts that a strictly software implementation is directed toward non-statutory subject matter. It is not clear what the Examiner means by a "strictly software implementation" or what section of the MPEP is being used for the rejection. Software by itself does not compute anything, only once the instructions of the software are used to configure the hardware of a circuit (such as a processor) can the calculations be performed.

Claim 14 recites "*an integrated circuit configured to compute the number of points on an elliptic curve.*" Because claim 14 is directed to a circuit that does compute the number of points and because only hardware can actually compute values, the claimed "logic" inherently has to be hardware. The hardware may be application specific (e.g. an ASIC), may be configurable (e.g. an FPGA) with configuration data, or the hardware may be a general purpose processor, which is configured by software instructions. Thus, the claim necessarily includes hardware, although the hardware may be configured with software. Therefore, as the claims are directed to a circuit that is actually configured to compute the number of points on the curve, claim 14 is directed to a hardware implementation, and is thus directed to patentable subject matter.

For at least these reasons, Applicant respectfully requests the withdrawal of this rejection.

Objection to the Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter of "a computer-readable medium." Paragraph 40 has been amended to add the term "computer readable" to the phrase "re-programmable computer readable media." Given the context of the paragraph (e.g. recitation of a "general-purpose computing environment"), one skilled in the art would have recognized that the media would be computer readable. Accordingly, this amendment is supported.

For at least these reasons, Applicant respectfully requests the withdrawal of this objection.

Claim Rejections under 35 USC § 112, first paragraph

Claims 12, 13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement because the term "readable medium" does not appear within the specification or the original claims.

Although the term "readable medium" is not used in the specification, the original paragraph 40 of the present specification did recite the term "re-programmable media." The MPEP § 2163.02 states that the subject matter need not be "described literally (i.e. using the same terms …)." Thus, original paragraph 40 of the specification (version available on PAIR) does describe the subject matter of claim 12 to satisfy the written description requirement.

For at least these reasons, Applicant respectfully requests the withdrawal of this rejection.

Claim Rejections under 35 USC § 112, second paragraph

Claims 1, 12, 14 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The Office Action states that "[t]here is no disclosure within the specification or the original claim for the following claim limitation '*determining the number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision.*'" The Office Action also states that there is no disclosure for the term "*lifted Frobenius*".

Although the rejection states that 35 U.S.C. 112, second paragraph, is being used, the language of the rejection (e.g. that no disclosure exists) suggest that the rejection is actually based on 35 U.S.C. 112, first paragraph. Applicants request clarification.

Paragraph 4 states "[t]he present invention relates to … the computation of the number of points on elliptic curves … ." Accordingly, the specification does disclose computing the number of points on a curve. Furthermore, the Office Action points out that the specification does state "a second phase computes a norm to determine the number of points on the curve as output." Thus, the specification does very clearly disclose the determining step.

As to the term "lifted Frobenius," paragraph 9 states "a first phase lifts an elliptic curve given as input in order to determine certain intermediate quantities." Also, paragraph 11 states "[t]he p-adic algorithms known in the art permit lifting of elliptic curves …." One skilled in the art (e.g. one familiar with lifted Frobenius equations) knows that the lifting of an elliptical curve involves solving a lifted Frobenius equation. *See* references Sat2000 and FGH2000 as provided in paragraph 19 of the present specification. Paragraphs 31-32 specifically describe the lifted Frobenius equation that involves a Frobenius operator that involves a lift of the polynomials. Accordingly, the specification does disclose a "lifted Frobenius equation."

As to the full and reduced precision, paragraph 17 discloses an example of how the different precisions are used. At cols. 5 and 6, U.S. Patent 7,308,469 by the Applicant provides a general description about the term "precision" as it would be understood by one skilled in the art. Thus, such limitations are supported and definite as being a common term in the field.

Accordingly, Applicant respectfully requests the withdrawal of this rejection.

Claim Rejections under 35 USC § 103(a), Hoffstein, Gressel, Penner

Claims 1-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hoffstein et al. (US Patent No. 7,031,468) in view of Gressel et al. (US Patent No. 6,748,410) and further in view of Penner (US Patent No. 7,158,569).

Claims 1-11

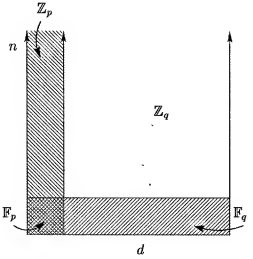
Claim 1 is allowable over the cited references, either alone or in combination, as those references fail to teach or suggest all the elements of claim 1. For example, claim 1 recites:

receiving an elliptic curve having a total number of points on the entire curve; and

determining the total number of points on the elliptic curve, wherein the determining includes solving a lifted Frobenius equation to a full precision by using first and second parts with a reduced precision.

Hoffstein describes a method for computing multiples of points (e.g. element A) on an elliptic curve. *See Hoffstein*, col. 3 line 37 to col. 4 line 41. Thus, Hoffstein is able to only determine specific points on the elliptic curve that are related as multiples. Such a method does not provide a way to count all of the points of a curve. There are far too many points on any non-trivial curve to be able to consider individual points. Thus, Hoffstein does not disclose determining the total number of points on an entire elliptic curve. As the cited teachings of the other references do not make up for this deficiency in Hoffstein, any combination of these references do not teach or suggest "*determining the total number of points on the elliptic curve,*" as recited in claim 1.

As to a lifted Frobenius equation, the arguments above show that a lifted Frobenius equation is disclosed in the present specification. For further clarification, the figure below is provided.



In the above figure, Z_p is the p-adic integers (to precision n); F_p is the Galois field of integers modulo a prime p; F_q: the degree-d Galois extension of F_p; and Z_q is the degree-d Galois extension of Z_p (to precision n).

The first three (Z_p, F_p, F_q) are standard in arithmetic and elliptic curves. The last (Z_q) only recently became of interest in tangible applications, since the discovery described in references [Sat2000], [FGH2000]. See table 1 of the original patent application. In F_p and Z_p , the Frobenius operation is the identity, and thus does nothing. In F_q, the Frobenius operation is a simple p-th powering operation, as is done in Hoffstein. However, in Z_q, the Frobenius operation is a complex operation, which makes solving equations involving it particularly challenging. The act of lifting the operation from F_q into Z_q is used by those skilled in the art to refer to the lifted Frobenius equation.

Hoffstein explicitly and repeatedly say that the Frobenius they use is "the p-power Frobenius" on GF(q), i.e., on the Galois field as denoted F_q, and is not the lifted Frobenius on Z_q. *See Hoffstein*, col. 3 lines 54-67. Thus, Hoffstein does not disclose "*solving a lifted Frobenius equation,"* as recited in claim 1. As the cited teachings of the other references do not make up for this deficiency in Hoffstein, any combination of these references do not teach or suggest this claim element.

For at least these reasons, claim 1 is allowable over the cited references. As claim 1 is allowable, claims 2-11 which depend therefrom are also allowable for at least the same rationale.

Claims 3 and 4

In addition to being allowable for the same rationale as claim 1, claims 3 and 4 are allowable for additional reasons. For example, claim 3 recites "*in which said first and second parts compute the Teichmüller lift of a given finite-field polynomial.*" For example, claim 4 recites "*in which said first and second parts compute the canonical lift of said elliptic curve.*"

At pages 13 and 14, the Office Action states that Penner discloses computing a Teichmuller lift and a canonical lift. The cited section of Penner simply use the term "canonical"

for equations involving wavelets. There is not use of the term "lift" nor "elliptical curve." Penner's use of the term "canonical" is completely unrelated to lift of an elliptical surve.

Similarly, Penner used the term "Teichmuller" in reference to a book on hyperbolic geometry. Again, there is no mention of the term "lift" or any type of operation on a finite-field polynomial. Penner only mentions the title of the book, and no Teichmuller operations of any kind. These citations are simply a use of one word in a claim element, which are unrelated to a "lift" operation as is recited in claims 3 and 4.

For at least this additional reason, claims 3 and 4 are allowable over the cited references.

Claims 12-15

Applicants submit that independent claims 12 and 14 should be allowable for reasons mentioned with respect to claim 1. As claim 12 is allowable, dependent claim 13 is allowable for at least the same rationale. As claim 14 is allowable, dependent claim 15 is allowable for at least the same rationale.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 415-576-0200.

Respectfully submitted,

/David B. Raczkowski/

David B. Raczkowski
Reg. No. 52,145

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 415-576-0200
Fax: 415-576-0300
DBR:scz
61338001 v1